Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 19 June 2014

Public Authority: Chief Constable of Derbyshire Constabulary
Address: Police Headquarters
Butterley Hall
Ripley
Derbyshire
DE5 3RS

Decision (including any steps ordered)

1. The complainant requested all IP addresses used by Derbyshire Constabulary to access the internet. The Constabulary refused to disclose this information under the exemptions provided by the following sections of the FOIA:

   24(1) (national security)

   31(1)(a) (prejudice to the prevention or detection of crime)

   31(1)(b) (prejudice to the apprehension or prosecution of offenders)

2. The Commissioner's decision is that Derbyshire Constabulary cited section 31(1)(a) correctly and so it was not required to disclose this information.

Request and response

3. On 30 October 2013, the complainant wrote to Derbyshire Constabulary and requested information in the following terms:

   "Under the Freedom of Information Act please disclose all IP addresses used by your constabulary to access the internet. In the case of

dynamic IP addresses please give details of the server and / or host including its location which assigns them."

4. Derbyshire Constabulary responded on 7 November 2013. It stated that the request was refused and cited the exemptions provided by sections 24(1) (national security) and 31(1)(a) and (b) (prejudice to the prevention or detection of crime and to the apprehension or prosecution of offenders) of the FOIA.

5. The complainant responded on the same date and requested an internal review. The complainant argued at this stage that other police forces had disclosed similar information.

6. Derbyshire Constabulary responded with the outcome of the internal review on 20 November 2013. The conclusion of this was that the refusal under sections 24(1), 31(1)(a) and 31(1)(b) was upheld.

Scope of the case

7. The complainant contacted the Commissioner on 20 November 2013 to complain about the refusal of his information request. The complainant indicated at this stage that he did not agree with the reasoning given by the Constabulary for the refusal of his request.

8. During the Commissioner's investigation, the Constabulary disclosed to the complainant the IP address of its website. This analysis covers the remaining IP addresses, none of which were disclosed.

Reasons for decision

Section 31(1)(a)

9. The Commissioner has focussed first on this exemption, which provides that information is exempt where its disclosure would, or would be likely to, prejudice the prevention or detection of crime. Consideration of section 31(1)(a) is a two-stage process. First, the exemption must be engaged as prejudice to the prevention or detection of crime would be at least likely to result through disclosure. Secondly, this exemption is qualified by the public interest, which means that the information must be disclosed if the public interest in the maintenance of the exemption does not outweigh the public interest in disclosure.

10. The Commissioner has considered here whether prejudice *would be likely* to result, rather than whether it *would* result. The test that the Commissioner applies when considering whether prejudice would be

likely is that there must be a real and significant, rather than hypothetical or remote, chance of the prejudice occurring.

11. The argument of the Constabulary here was essentially that disclosure of IP addresses would be likely to result in harm to its IT systems, in turn prejudicing the Constabulary's ability to carry out its role of crime prevention and detection. The Commissioner recognises that this argument is relevant to section 31(1)(a). The next step is to consider whether the level of likelihood of this prejudice occurring meets the test of real and significant.

12. The Constabulary argued that disclosure of its IP addresses would render its IT system vulnerable to various forms of attack, including denial of service attacks. The key question is, therefore, whether disclosure would render the Constabulary's systems vulnerable in the way suggested.

13. The Commissioner would note first that he accepts that there are individuals and groups who would be likely to take advantage of an opportunity to disrupt the Constabulary's systems. As to whether it would be possible to use the requested IP addresses for such disruption, the view of the Commissioner is that the wording of the request means that it covers both private and public IP addresses.

14. A private IP address (sometimes called a local IP address) is one with a specific range that has been reserved for use of a private network and cannot be accessed from the internet. A public IP address is one that is publically addressable from the internet and is not in a reserved range.

15. Publicly searchable databases exist which permit individuals to view which organisation a public IP address has been allocated to. However, this does not mean that that same organisation is operating the device to which that IP address is allocated. For example, Cable and Wireless have been allocated a wide range of IP addresses. It would not, however, be known which, if any, of these were being used by Derbyshire Constabulary.

16. In some instances it is critical that the IP address is public knowledge – the IP address of a public facing website for example. As noted above at paragraph 8, the Constabulary disclosed to the complainant the IP address of its website.

17. However, if a device is offering a service specifically for the internal use of the Constabulary, the public IP address may not be widely known. If it is known that a specific public IP address, or range of addresses, are used by a particular organisation or offer a particular type of service then they could be used to direct efforts to attack those systems. For

example, a flood of traffic could be directed at a specific IP address in order to mount a denial of service attack. This could have the effect of making the service no longer responsive or accessible for its intended purpose.

18. As to private IP addresses, if these were disclosed they would reveal the existence of services within the private network. This knowledge could be of use to an attacker but generally only once they had first defeated the perimeter defences.

19. As mentioned above, when making his complaint to the Commissioner, the complainant stated that other police forces had disclosed similar information. The one disclosure that the Commissioner is aware of was carried out by the Metropolitan Police Service (MPS). This was a very limited disclosure of two IP addresses, and appears to have been based on a narrower reading of the request than the Commissioner has applied here. In any event, previous disclosures do not preclude the Commissioner from reaching any particular conclusion in this case.

20. In summary, the Commissioner accepts that there are those who would seek to disrupt the Constabulary's IT systems and that disclosure of the withheld IP addresses could be used for such disruption. Furthermore, he also accepts that a significant disruption of the Constabulary's IT systems would be likely to also disrupt its work in preventing and detecting crime.

21. For these reasons, the Commissioner's conclusion is that there would be a real and significant likelihood of prejudice to the prevention or detection of crime resulting through disclosure of the information in question, and so the exemption provided by section 31(1)(a) of the FOIA is engaged.

22. The next step is to consider the balance of the public interest. In reaching a conclusion here, the Commissioner has taken into account the general public interest in Derbyshire Constabulary being open and transparent, as well as the specific factors that apply in relation to the information in question.

23. Covering, first arguments against disclosure, appropriate weight must be afforded here to the public interest inherent in the exemption; that is, the public interest in avoiding likely prejudice to the prevention or detection of crime by the Constabulary. The Commissioner considers it clear that there is a very substantial public interest in avoiding that outcome and that this is a public interest factor in favour of maintenance of the exemption of considerable weight.

24. Turning to factors that favour disclosure of this information, other than the general public interest in the Constabulary being open and transparent that is referred to above, the Commissioner is of the view that there is little public interest in the disclosure of the specific information in question here, which is a list of IP addresses. The argument advanced by the complainant was that this information should be disclosed as it had been by other police forces. However, as already covered above, the only disclosure by another force that the Commissioner is aware of was that by the MPS. Whilst the Commissioner is not aware of the precise reasoning of the MPS for disclosing that information, he does not regard it as indicative of a strong public interest in police IP addresses.

25. In the absence of public interest factors in favour of disclosure relating to the specific information in question, the Commissioner has weighed the public interest in avoiding prejudice to the prevention or detection of crime against the public interest in the openness and transparency of the Constabulary. His conclusion is that the public interest in avoiding prejudice is the more weighty factor and so his finding here is that the public interest in the maintenance of the exemption outweighs the public interest in disclosure.

26. Derbyshire Constabulary was not, therefore, required to disclose this information. Given this finding it has not been necessary for the Commissioner to go on to consider the other exemptions that were cited by the Constabulary.

Right of appeal

27. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0116 249 4253
    Email: GRC@hmcts.gsi.gov.uk
    Website: http://www.justice.gov.uk/tribunals/general-regulatory-chamber

28. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

29. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Steve Wood
Head of Policy Delivery
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF